Firewall Log Analyzer and Monitoring Tool

1. Project Overview

The Firewall Log Analyzer and Monitoring Tool is a cybersecurity application designed to collect, analyze, and monitor firewall logs in real time to detect suspicious activities and potential cyberattacks. It automates the analysis of large firewall log files and presents meaningful insights through a web-based dashboard.

2. Problem Statement

Firewall logs are generated continuously and are difficult to analyze manually. This leads to delayed threat detection and inefficient security monitoring. The project provides an automated solution for log analysis and threat identification.

3. Objectives

- Analyze firewall logs automatically

- Detect suspicious and malicious activities

- Provide real-time monitoring and alerts

- Store logs securely for future reference

- Generate filtered reports

4. System Architecture

Firewall logs are collected and sent to the backend analyzer. The backend processes the logs, detects threats, stores results in MongoDB, and displays insights on a React-based dashboard. Alerts are sent via email and reports can be exported as PDF.

5. Key Features

- Suspicious traffic detection

- Brute force and port scanning detection

- SQL and SSH access monitoring

- Real-time dashboard

- Date and time filters

- Email alerts

- PDF report generation

6. Technology Stack

Frontend: React.js, HTML, CSS

Backend: Python , ML-based detection

Database: MongoDB

Security Tools: Firewall logs, Email alerts(optional)

7. Applications

- Network security monitoring

- Educational institutions

- Enterprise security systems

8. Future Enhancements

- Live firewall rule blocking

- Advanced ML attack detection

- Geo-location tracking of IPs

9. Conclusion

The project improves network security by automating firewall log analysis and providing real-time threat monitoring.